REMARKS

Claims 1-5, 8-16, 19-25, 28-34, 37-43, 46-52 and 55-63 are pending in the present application, of which claims 1, 5, 9, 13, 16, 19, 22, 25, 28, 31, 34, 37, 40, 43, 46, 49, 52, 55, 58, 60 and 62 are independent. No amendments have been made. Applicants believe that the present application is in condition for allowance, which prompt and favorable action is respectfully requested.

REJECTION UNDER 35 U.S.C. §102

The Examiner rejected claims 1-5, 8-16, 19-25, 28-34, 37-43, 46-52 and 55-63 under 35 U.S.C. §103 as being unpatentable over U.S. Patent Re. 33,189 issued to Lee et al. (hereinafter "Lee") in view of Handbook of Applied Cryptography by Menezes et aL (hereinafter "Menezes"). Applicants respectfully disagree and request the Examiner to reconsider the rejection in light of the remarks set forth below.

> To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the reference themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim elements. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure. (MPEP 2143)

Lee discusses a security subsystem for a subscription television system. Particularly, Lee teaches storing subscriber information including user specific ID codes. The user specific ID codes are set prior to installation and stored in various subscriber units. To protect TV signal transmission from unauthorized reception, Lee teaches encrypting a program signal based on a PN sequence segment, wherein a random number and a key loaded into a PN sequence generator to periodically seed the generator. The key is encrypted based a user specific ID code and sent to a subscriber receiver of the corresponding user. Also, the random number is encrypted based on the key and sent to the subscriber receiver. (See col. 3, lines 30-60 and lines 67-69).

The subscriber receiver, having already stored the user specific ID code, receives the encrypted key, the encrypted random number and the encrypted/scrambled program signal. The key is recovered based on the user specific ID code and the random number is recovered based on the recovered key. Thereafter, the key and the random number are used to generate the PN sequence segment in order to descramble the received program signals. (See col. 4, lines 1-22). As such, Lee teaches sending of a key by which only the subscribed user can descramble the program signals. Lee does not teach or even suggest a key exchange.

In the rejection, the Examiner seems to equate the public key with either the key or the user ID of Lee, the secret key with either the key or the user ID of Lee, and the access key with the random number.

However, as described above, the random number does not function as a key, but as a seed to reset the PN sequence generator. Moreover, in Lee, since the user ID is a pre-shared secret, it must be provisioned in the subscriber receiver at installation and, as a secret, cannot be distributed. Accordingly, if the public key is equated with the user ID, only for purposes of argument, Lee does not teach or disclose distributing the user ID as in claims 1, 22, 40 and 58. If the public key is equated with the key of Lee, also only for purposes of argument, Lee does not teach or disclose both secret key and an access key. Additionally, in either case, Lee does not teach both distributing and receiving keys as in claims 1, 22, 40 and 58.

With respect to claims 5, 25, 43 and 60, the Examiner seems to be equating the public key with key/user ID and broadcast access key with the key. If the public key is equated with the user ID, only for purposes of argument, Lee does not teach or disclose distributing the user ID as in claims 5, 25, 43 and 60. If the public key is equated with the key of Lee, also only for purposes of argument, Lee does not teach or disclose the broadcast key. Additionally, in either case, Lee does not teach both distributing and receiving keys as in claims 5, 25, 43 and 60.

With respect to claims 9, 28, 46 and 62, the Examiner seems to be equating the public key with key/user ID, the secret key with either the key/user ID of Lee, and the access key with the random number. If the public key is equated with the user ID, only for purposes of argument, Lee does not teach or disclose receiving the user ID as in claims 9, 28, 46 and 62, since the user ID is already provisioned. If the public key is equated with the key of Lee, also only for purposes of argument, Lee does not teach or disclose both a secret key and an access key. Additionally, in either case, Lee does not teach both receiving and sending of keys as in claims 9, 28, 46 and 62.

With respect to claims 13, 31 and 49, the Examiner seems to be equating the public key with key/user ID, the secret key with the key of Lee, and the access key with the random number. If the public key is equated with the user ID, only for purposes of argument, Lee does not teach or disclose receiving the user ID as in claims 13, 31 and 49, since the user ID is already provisioned. If the public key is equated with the key of Lee, also only for purposes of argument, Lee does not teach or disclose both a secret key and an access key. Additionally, in either case, Lee does not teach both receiving and sending of keys as in claims 13, 31 and 49.

With respect to claims 16, 34 and 52, the Examiner seems to be equating the public key with key/user ID and broadcast access key with the key. If the public key is equated with the user ID, only for purposes of argument, Lee does not teach or disclose receiving the user ID as in claims 16, 34 and 52. If the public key is equated with the key of Lee, also only for purposes of argument, Lee does not teach or disclose the broadcast key. Additionally, in either case, Lee does not teach both receiving and sending keys as in claims 16, 34 and 52.

With respect to claims 19, 37 and 55, the Examiner seems to be equating the public key with key/user ID, the secret key with the key of Lee, and the access key with the random number.

If the public key is equated with the user ID, only for purposes of argument, Lee does not teach or disclose distributing the user ID as in claims 19, 37 and 55, since the user ID is a secret. If the public key is equated with the key of Lee, also only for purposes of argument, Lee does not teach or disclose both a secret key and an access key. Additionally, in either case, Lee does not teach both distributing and receiving of keys as in claims 19, 37 and 55.

Furthermore, with respect to the independent claims above, the Examiner admitted that Lee fails to disclose or suggest a public key, but relied upon Menezes to allegedly cure this deficiency. Particularly, the Examiner states that Menezes teaches key layering is a key-exchange technique. Applicants respectfully disagree with the characterization of the cited portions of Menezes.

In the cited portion, Menezes discusses public-key encryption and key layering. Particularly, Menezes teaches using a master key K_M to distribute a session key to various terminals X and Y (See page 552, section 13.9). As such, Menezes, at most, teaches distributing a key using a key layering technique and does not teach an exchange of keys. Accordingly, assuming that the teachings of Menezes can be combined with Lee, a key exchange as in claims 1, 5, 9, 13, 16, 19, 22, 25, 28, 31, 34, 37, 40, 43, 46, 49, 52, 55, 58, 60 and 62 is not disclosed. Therefore, Applicants respectfully submits that the Examiner has failed to set forth a prima facie case of obviousness.

Also, claims 2-4, 8, 10-12, 14-15, 20-21 23-24, 29-30, 32-33, 38-39, 41-42, 47-48, 50-51, 56-57, 59, 61, and 63 depend from and include all the elements cited in the independent claims 1, 5, 9, 13, 16, 19, 22, 25, 28, 31, 34, 37, 40, 43, 46, 49, 52, 55, 58, 60 and 62, respectively. Therefore, Applicants submit that these claims are believed to be allowable based on their dependency from an allowable base claim as well as other novel features included therein.

Since neither Lee nor Menezes, separately or combined, teach or suggest the claimed subject matter, Applicants respectfully request a withdrawal of the rejection under 35 U.S.C. §103, for at least the foregoing reasons.

CONCLUSION

In light of the amendments contained herein, Applicants submit that the application is in condition for allowance, for which early action is requested.

Please charge any fees or overpayments that may be due with this response to Deposit Account No. 17-0026.

Respectfully submitted,

Dated: November 30, 2005

By: ______________________
Jae-Hee Choi, Reg. No. 45,288
(858) 658-5469

QUALCOMM Incorporated
Attn: Patent Department
5775 Morehouse Drive
San Diego, California 92121-1714
Telephone: (858) 658-5787
Facsimile: (858) 658-2502